DOCUMENT RESUME

ED 275 349 IR 051 697

TITLE	Privacy Act. Federal Agencies' Implementation Can Be Improved. Report to the Chairman, Subcommittee on Government Information, Justice, and Agriculture, Committee on Government Operations, House of Representatives.
INSTITUTION	General Accounting Office, Washington, D.C.
REPORT NO	GAO/GGD-86-107
PUB DATE	Aug 86
NOTE	62p.
AVAILABLE FROM	General Accounting Office, PO Box 6015, Gaithersburg, MD 20877 (first 5 copies free, additional copies, $2.00 each).
PUB TYPE	Legal/Legislative/Regulatory Materials (090) -- Reports - Research/Technical (143)
EDRS PRICE	MF01/PC03 Plus Postage.
DESCRIPTORS	Access to Information; Automation; *Compliance (Legal); Disclosure; Federal Government; *Federal Regulation; Information Dissemination; Information Storage; Information Systems; Legislation; *Privacy; *Public Agencies; Recordkeeping
IDENTIFIERS	Office of Management and Budget; *Privacy Act 1974

ABSTRACT

In order to examine the implementation of the Privacy Act of 1974 by federal government agencies, the General Accounting Office (GAO) examined organizational issues at 13 cabinet-level departments and the Veterans Administration and reviewed Privacy Act operations in detail at 6 of these agencies and 37 of their components. This study focused on how the agencies have (1) organized their Privacy Act activities, and (2) followed selected provisions of the Act and Office of Management and Budget (OMB) guidelines. GAO found that agencies have taken highly decentralized approaches to implementing the law, and often have not established clear lines of responsibility and accountability for Privacy Act functions. As a result of the study, GAO made a number of recommendations to the OMB for improvement in oversight, agency evaluation, and certain OMB guidelines pertaining to such activities as computer matching programs. Supporting material is provided in three tables and three appendices; a glossary is also included. (KM)

****
* Reproductions supplied by EDRS are the best that can be made *
* from the original document. *
****

ED275349

United States General Accounting Office

GAO

Report to the Chairman, Subcommittee on Government Information, Justice, and Agriculture, Committee on Government Operations
House of Representatives

August 1986

U.S. DEPARTMENT OF EDUCATION
Office of Educational Research and Improvement
EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)

☑ This document has been reproduced as received from the person or organization originating it.

☐ Minor changes have been made to improve reproduction quality.

• Points of view or opinions stated in this document do not necessarily represent official OERI position or policy.

PRIVACY ACT

Federal Agencies' Implementation Can Be Improved

BEST COPY AVAILABLE

IR051697

GAO/GGD-86-107

GAO

United States
General Accounting Office
Washington, D.C. 20548

General Government Division

B-223140

August 22, 1986

The Honorable Glenn English
Chairman, Subcommittee on Government
Information, Justice, and
Agriculture
Committee on Government Operations
House of Representatives

Dear Mr. Chairman:

This report is in response to your request that we examine how federal agencies have implemented the Privacy Act of 1974. The report addresses the organizational structures adopted by agencies, the roles of agency Privacy Act officers, and agency adherence to Privacy Act provisions and Office of Management and Budget (OMB) guidance.

As arranged with your office, unless you publicly announce the contents of the report earlier, we plan no further distribution until 30 days from the date of the report. At that time we will send copies to OMB, the Cabinet departments and the Veterans Administration, congressional committees having an interest in privacy-related matters, and other interested parties. Additionally, we will make copies available to others upon request.

Sincerely yours,

W. J. Anderson

William J. Anderson
Director

Executive Summary

Purpose

Federal agencies collect and use virtually billions of records containing personal information on individuals. The possession of such vast quantities of personal information has raised public and congressional concerns over the ability to protect and balance the privacy of individuals in relation to the information needs of government. This concern has grown as expanding information technologies are providing for faster, broader, and less expensive access to these sensitive records.

GAO was requested by the Chairman, Subcommittee on Government Information, Justice, and Agriculture, House Committee on Government Operations, to examine agencies' implementation of the Privacy Act of 1974, the principal law aimed at protecting personal privacy. This report provides an analysis of how agencies have (1) organized their Privacy Act activities and (2) followed selected provisions of the act and Office of Management and Budget (OMB) implementing guidelines.

Background

The Privacy Act of 1974 provides certain safeguards to individuals against invasion of privacy by requiring federal agencies to establish rules and procedures for maintaining and protecting personal data in agency record systems.

A basic premise of the law is that information about individuals should not be maintained in secret files. With some exceptions, individuals have the right to (1) know what records pertaining to them are collected, maintained, used, and disseminated by the agencies; (2) have access to agencies' information pertaining to them and to amend or correct the information; and (3) prevent information obtained by agencies for a specific purpose from being disclosed for another purpose without their consent.

The act also requires agencies to insure that any records of identifiable personal information they maintain are for necessary and relevant purposes, that they are current and accurate for their intended uses, and that adequate safeguards are provided to prevent misuse of such information. Each agency is responsible for implementing the act with guidance and oversight from OMB. (See pp. 8 to 10.)

GAO examined organizational issues at 13 Cabinet-level departments and the Veterans Administration and reviewed Privacy Act operations in detail at six of these agencies and 37 of their components.

Results in Brief

Agencies have taken highly decentralized approaches to implementing the law and often have not established clear lines of responsibility and accountability for Privacy Act functions. All of the 14 agencies had Privacy Act officers or their equivalent; however, the officers' limited responsibilities and resources indicated that they did not exercise the oversight originally envisioned by OMB. At the six agencies GAO reviewed in detail, improvements were needed in adhering to OMB guidance relating to such activities as computer matching programs, risk assessments, evaluations, and training.

Clearer Responsibility and Accountability Needed

The degree to which Privacy Act responsibilities were clearly delineated and accountability established varied widely among the agencies. Three of the 14 agencies did not have agencywide directives specifying responsibilities. The other 11 agencies had published directives, but they generally lacked detail and specificity. For example, Privacy Act functions such as computer matching, compliance evaluations, and training were frequently not addressed in the directives. (See pp. 15 to 17.)

Privacy Act Officers Have Limited Roles

The position of Privacy Act officer was established to provide coordination and oversight of Privacy Act implementation. GAO's analysis of agency directives and position descriptions, however, showed that significant functions such as ensuring compliance and providing Privacy Act training were not always assigned. Even if these and other responsibilities were assigned, it is doubtful that the Privacy Act officers could carry them out given the resources made available to them. These individuals generally held mid-level management positions and conducted Privacy Act activities on a part-time basis, in 10 agencies less than half-time. Five officers had no staff resources. Of the nine who had assistants, seven had fewer than the full-time equivalent of 1 staff. (See pp. 18 to 22.)

Many Improvements Needed at the Six Agencies Reviewed in Detail

While OMB asks agencies to conduct detailed risk assessments for newly created or modified record systems to assure security and confidentiality, the six agencies in GAO's detailed review could provide evidence of an assessment for only 1 of 27 record systems. Five of the six agencies did not report accurate data to OMB on the extent of their computer matching activities. In addition, of 26 computer matching programs, 6 did not follow OMB guidance. The training needs of the hundreds of individuals responsible for Privacy Act compliance had not been assessed or provided in a systematic manner. The agencies did not routinely conduct

internal evaluations of Privacy Act operations. Where matching and other activities related to the Privacy Act were conducted, Privacy Act officers at both agency and component levels were frequently unaware of and uninvolved in them. (See ch. 3.)

Recommendations

Because of OMB's key role in managing executive branch operations and in light of the responsibilities assigned to it by the Privacy Act, GAO makes a number of recommendations to OMB for improvement in oversight, agency evaluation, and OMB guidelines pertaining to such activities as computer matching programs. (See pp. 48 to 49.)

Agency Comments

OMB said it believes GAO's recommendations are reasonable and has been working to implement some of them. OMB's other comments concerned such areas as the Paperwork Reduction Act, the role of Privacy Act officers in relation to senior officials, and the impact of concurrent responsibilities on Privacy Act officers' duties. (See pp. 49 to 50.)

Contents

Executive Summary		2
Chapter 1 Introduction		8
	Agencies' Responsibilities Under the Privacy Act	8
	The Role of the Office of Management and Budget	10
	Objectives, Scope, and Methodology	12
Chapter 2 Agencies Need to Better Define Privacy Act Responsibilities		14
	Privacy Act Responsibilities Are Highly Dispersed Throughout the Agencies	14
	Improved Directives Are Needed to Communicate Privacy Act Responsibilities	15
	Role of Departmental Privacy Act Officer Needs to Be Reexamined	18
	Privacy Issues Not Covered by the Act	22
Chapter 3 Experiences of Six Agencies Show Improvements Are Needed		24
	Detailed Risk Assessments Were Not Conducted or Were Not Available for New and Revised Systems of Records	25
	Agency Automation of Systems of Records	27
	Improvements Can Be Made in Overseeing Computer Matching	29
	Agencies Need to Better Monitor Privacy Act Training	40
	Agencies Need to Evaluate Privacy Act Activities	41
Chapter 4 Conclusions and Recommendations		46
	Conclusions	46
	Recommendations	48
	Agency Comments and Our Evaluation	49
Tables		
	Table 2.1: Functions Assigned to Privacy Act Officers by 14 Agencies	19
	Table 2.2: Location and Resources of Agency Privacy Act Officers and Staff	20
	Table 3.1: 1983 Computer Matching Programs at Six Agencies	32

Appendixes

Appendix I: Letter Dated January 4, 1984, From the Chairman of the Subcommittee on Government Information, Justice, and Agriculture 52
Appendix II: Location and Resources of Component Privacy Act Staff 54
Appendix III: Comments From the Office of Management and Budget 57
Glossary 59

Abbreviations

BOP	Bureau of Prisons
DOD	Department of Defense
GAO	General Accounting Office
HHS	Health and Human Services
HUD	Housing and Urban Development
IRS	Internal Revenue Service
NASA	National Aeronautics and Space Administration
OCSE	Office of Child Support Enforcement
OGC	Office of General Counsel
OIG	Office of Inspector General
OMB	Office of Management and Budget
OTA	Office of Technology Assessment
PHS	Public Health Service
SSA	Social Security Administration
VA	Veterans Administration

Introduction

The Privacy Act of 1974 (Public Law 93-579) was enacted on December 31, 1974, and became effective on September 27, 1975. This legislation established governmentwide standards to protect the privacy of personal information. Because the government is one of the largest users of personal information, the Congress recognized the need to protect the ordinary individual from potentially abusive powers of government while ensuring that the government would have the information it needed to operate its many programs. In 1983, federal agencies reported maintaining about 4,700 systems of records that have been estimated to contain personal information on virtually everyone in the country.

After oversight hearings conducted in June 1983, the Chairman, Subcommittee on Government Information, Justice, and Agriculture, House Committee on Government Operations, requested that we review agencies' implementation of the Privacy Act of 1974. The 1983 hearings focused on OMB's responsibilities under the act for providing guidance and oversight to agencies.

Agencies' Responsibilities Under the Privacy Act

The Privacy Act provides safeguards against the misuse of personal information by requiring federal agencies to establish rules and procedures for maintaining and protecting personal data in agency record systems.

A basic premise of the law is that information about individuals should not be maintained in secret files. Agencies are required to publish in the Federal Register various data relevant to all of their systems of records containing information about individuals. A system of records is defined by the act as any group of records under the control of an agency from which information is retrieved by an individual's name or some identifying number or symbol or other identifying particular assigned to the individual. Information to be published in the Federal Register includes a description of the categories of records maintained, the types of sources for the information, and purposes of the records.

Upon request, an agency must permit the subject of a record to gain access to and copy the record. An individual disagreeing with the contents of the record may request it be amended. If the request is denied, or not satisfactorily resolved, the individual may appeal the decision to a higher level in the agency. Then, if the matter is still unresolved, the individual may appeal the matter to a district court and/or place a statement of disagreement in the record. The agency is required to distribute the statement of disagreement with all subsequent disclosures of the

record and to any person or agency to whom disclosures of the record have previously been made.

Individual records contained in a system of records may not be disclosed to others by an agency unless the subject of the record agrees or the disclosure is specifically permitted by the act. The act lists 12 categories of permissible disclosures, examples of which are: disclosures to agency employees who have a need for the record in the performance of their duties; disclosures to the Congress, the courts, and the General Accounting Office; and disclosures for a routine use. Routine use is defined in the act as the use of a record compatible with the purpose for which the record was collected. Routine uses must be described in the published descriptions of systems in the Federal Register.

Other provisions of the act require that agencies

- maintain only personal information that is relevant and necessary to accomplish a legal purpose of the agency;
- collect personal information to the greatest extent practicable directly from the subject when the use of the information may result in an adverse determination;
- inform each individual asked to supply personal information of the authority for the request, the principal purpose for which the information will be used, any routine uses, the consequences of failing to provide the requested information, and whether the disclosure is mandatory or voluntary;
- maintain records with such accuracy, relevance, timeliness, and completeness as are reasonably necessary to assure fairness when the information is disseminated;
- maintain no records describing how any individual exercises rights guaranteed by the First Amendment (religion, beliefs, or association) unless expressly authorized by statute or unless the records are pertinent to authorized law enforcement activities;
- establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records;
- sell or rent mailing lists only when specifically authorized by law; and
- promulgate rules to implement these provisions.

The act permits systems of records maintained by the Central Intelligence Agency and agencies involved in law enforcement to be exempted from many of its provisions. Other, more limited, exemptions are permitted for systems of records that contain classified information, statistical data, or information from confidential sources. The exemption

provisions, however, are not mandatory; they apply to a system of records only when specifically invoked by the head of an agency.

Agencies are subject to civil suit, and government employees may be penalized up to $5,000 when damages occur as a result of willful or intentional criminal action violating any individual's rights under the act.

The Role of the Office of Management and Budget

While each federal agency is primarily responsible for its implementation of the Privacy Act, the act makes OMB responsible for providing overall guidance, regulations, and oversight. The act also requires the President to submit an annual report, prepared by OMB, to the House and Senate giving a consolidated view of Privacy Act activities of the federal agencies. OMB's oversight role is also included in the Paperwork Reduction Act of 1980. This act provides a framework to aid federal agencies in the management of information resources and cites that the privacy functions of OMB include monitoring compliance with the Privacy Act.

OMB Guidelines and Other Instructions

The Privacy Act authorizes OMB to issue regulations for agencies to follow; however, OMB has chosen to limit its instructions to guidelines and circulars, having a somewhat less authoritative effect than regulations. Examples of OMB's guidelines and circulars follow.

- In July 1975, OMB issued Privacy Act Implementation Guidelines—a section-by-section discussion of the act and its requirements with references to the act's legislative history. OMB delegated responsibility for issuing additional guidance on specific Privacy Act subjects to other agencies. For example, the Secretary of Commerce (National Bureau of Standards) was delegated responsibility for issuing standards and guidelines on computer security.
- Also in July 1975, OMB published Circular No. A-108, Responsibilities for the Maintenance of Records About Individuals by Federal Agencies. This circular defined agency responsibilities for implementing the act, including meeting the publication requirements, providing adequate safeguards over personal records, and establishing a program for periodically reviewing policies and practices to assure compliance with the act.
- In March 1979, OMB issued Guidelines for the Conduct of Matching Programs which instructed agencies on how to collect, maintain, and disclose personal information when using a computer to identify

individuals whose records appear in more than one set of records. In May 1982, OMB revised the guidelines. It eliminated some provisions such as conducting cost/benefit analyses before conducting a computer matching program. It also added provisions such as instructing agencies to enter into written agreements with other participating agencies outlining how systems of records would be protected in matching programs.

- In December 1985, OMB issued Circular No. A-130, Management of Federal Information Resources. This circular, a general policy framework for information management, superseded Circular No. A-108 and replaced it with Appendix I entitled Federal Agency Responsibilities for Maintaining Records About Individuals. The appendix restated agency responsibilities and specified in greater detail the type and frequency of reviews that agencies need to conduct to ensure compliance with the Privacy Act.
- In February 1986, OMB announced its intention to comprehensively review and update its Privacy Act guidance. It requested suggestions for needed changes from Privacy Act experts and practitioners. OMB plans to publish revised guidelines for public comment in December 1986.

Oversight Provided by OMB

The Privacy Act also assigned OMB the responsibility to provide continuing assistance to and oversight of the act's implementation by the agencies. In meeting this responsibility, OMB (1) reviews agency reports on systems of records, computer matching programs, and other activities as provided for by the act or OMB instructions and (2) prepares the President's annual report to the House and Senate.

OMB's oversight approach was criticized in 1983 hearings held by the House Subcommittee on Government Information, Justice, and Agriculture.[1] The Subcommittee's report pointed out that, for example, "nothing in the Act indicates that a review of new or altered systems of records was intended to be the only type of OMB oversight . . . ." The report also stated that such efforts are essentially reactive which means that ". . . there is no monitoring by OMB of agency compliance with provisions of the law not reflected in the system reports."

The Subcommittee also criticized OMB's preparation of the 1980 and 1981 annual reports on agencies' implementation of the Privacy Act. The Subcommittee said the two reports were not as comprehensive as

[1]The Subcommittee report included two separate views by which some Subcommittee members expressed reluctance to criticize OMB's oversight approach because the act's legislative history was not clear as to what was expected. Despite their reluctance, those members expressed the view that OMB could do a more comprehensive job of overseeing agency compliance.

earlier reports. In 1982, OMB recommended that the Congress eliminate the Privacy Act annual report requirement and, instead, incorporate it into OMB's annual report under the Paperwork Reduction Act. The Congress rejected this proposal and instead expanded the report's contents. OMB's 1982 annual report, consolidated with the 1983 report, was published in December 1985. OMB was working on a consolidated 1984 and 1985 annual report when we completed our audit work in February 1986. OMB expected to issue the report in October 1986.

Objectives, Scope, and Methodology

We were asked to (1) review the organizational structure and effectiveness of Privacy Act implementation at major departments and agencies and (2) determine how major agencies are organized to permit identification and consideration of non-Privacy Act privacy issues in the ordinary course of agency business. In an earlier report, we responded to a third aspect of the request that pertained to the activity and resources devoted to privacy policy matters at the Department of Commerce's National Telecommunications and Information Administration. (GAO/GGD-84-93, Aug. 31, 1984)

To address the organizational issues, we conducted work at the 13 Cabinet-level departments and the Veterans Administration. At each of these agencies[2] we reviewed internal directives, orders, regulations, and other documents which establish and describe the organizational structure adopted for implementing the Privacy Act. We interviewed agency Privacy Act officers and other officials and obtained internal reports and other documents which also identified and described the roles and responsibilities of those assigned Privacy Act duties.

We selected for review three activities covered by the act and/or OMB guidelines. These activities included (1) creating new systems of records, (2) automating systems, and (3) computer matching. On the basis of the 1983 data available at the time we were planning our work, we selected 6 of the 14 agencies for more detailed analyses: the Departments of Health and Human Services, Interior, Justice, Labor, and Treasury, and the Veterans Administration. The six agencies accounted for 73 percent of all activity reported by the 14 agencies for the three activities selected. We also reviewed how the agencies conducted Privacy Act training and evaluated all Privacy Act operations. Although we did not review all the activities covered by the act—we excluded for example,

[2]For the purpose of this report, we refer to the 13 Cabinet-level departments and the Veterans Administration as agencies.

the access and amendment provisions—we believe our selection provides a range of activities sufficient to demonstrate (1) the roles and responsibilities of Privacy Act officers and (2) how effectively agencies have implemented provisions of the act and OMB guidance.

At the six agencies we reviewed in detail, we traced the 1983 activities pertaining to (1) creating new systems of records, (2) automating systems, and (3) computer matching through the procedural steps at the agency level as well as in 37 appropriate components. At each organizational level we reviewed internal documents and files and interviewed Privacy Act officers. In addition, we interviewed program personnel and staff from the offices of General Counsel, Inspector General, Personnel, Security, and others.

The request also asked how agencies identify and consider privacy issues not covered by the act. In consultation with the Subcommittee office, we limited our work on this question to interviews of agency Privacy Act officers at the 14 agencies. These privacy issues can be raised in a variety of contexts and are not necessarily related to systems of records issues which the Privacy Act covers.

We examined OMB's guidance to agencies, which included Circular Nos. A-108 and A-130, Privacy Act Implementation Guidelines, the 1979 Guidelines for the Conduct of Matching Programs, and the 1982 Guidance for Conducting Computer Matching Programs. We also reviewed 1983 hearings held by the House Subcommittee on Government Information, Justice, and Agriculture on OMB's oversight of the Privacy Act of 1974. We interviewed the OMB senior policy analyst who is the primary focal point for OMB's Privacy Act responsibilities to supplement this information.

We conducted our review from January 1985 to February 1986 in accordance with generally accepted government auditing standards. At the direction of the requester's office, we obtained comments on this report only from OMB.

Agencies Need to Better Define Privacy Act Responsibilities

The Privacy Act makes agency heads responsible for implementing and complying with its requirements. Because records are dispersed virtually throughout all agency components, agencies have adopted highly decentralized approaches to implementing the law. Decentralization makes it especially important that agency heads clearly assign responsibilities; however, the agencies varied in the degree to which they accomplished this. Clear lines of responsibility and accountability were not always established for Privacy Act functions.

Agencies have established a Privacy Act officer position to help coordinate Privacy Act matters—a critical position in a decentralized organization. However, some important functions such as ensuring compliance with Privacy Act provisions and OMB guidance had not been assigned to the Privacy Act officer. Even if such responsibilities were assigned, it is doubtful that the Privacy Act officers could carry them out effectively given the resources made available to them. Generally, these individuals (1) were mid-level employees, (2) had little or no Privacy Act staff to assist them, and (3) worked on Privacy Act activities on a part-time basis.

Agencies may engage in activities that have privacy implications outside the context of the Privacy Act. Most Privacy Act officers said that their agencies did not have a focal point or central mechanism to identify and address such issues, although such issues may be addressed by various organizational units as they arise.

Privacy Act Responsibilities Are Highly Dispersed Throughout the Agencies

Federal agencies maintain several thousand systems of records containing personal information on individuals. These records are used to administer federal programs and, as such, are maintained and operated by program staff in the many bureaus and offices at headquarters and in the field. Because the Privacy Act applies to each system of records regardless of location, Privacy Act functions are likewise widely dispersed and decentralized.

To illustrate, consider the structure of several agencies. The Department of Health and Human Services (HHS) reported that, as of 1983, it maintained 408 systems of records in its various components such as the Public Health Service, the Social Security Administration (SSA), and the Health Care Financing Administration. Within each component, systems of records were further decentralized. For example, the Public Health Service had 226 systems of records which were maintained by its various components such as the National Institutes of Health and the Food

and Drug Administration. The National Institutes of Health's 87 systems of records were further distributed among its 18 major components. Other agencies are similarly decentralized. The Veterans Administration (VA) and Justice, for example, reported for 1983 that they maintained 57 and 232 systems of records, respectively. These systems were dispersed throughout their many components and field offices. The Veterans Administration had, in addition to headquarters' divisions, several hundred facilities that had and used Privacy Act systems of records.

Just as agencies' systems of records are dispersed, so too are Privacy Act responsibilities. In addition to handling requests by individuals for access to their own records, Privacy Act responsibilities include other functions such as creating and modifying systems, ensuring that systems of records are adequately safeguarded, and participating in computer matching activities. Each function can involve people from different organizational components and organizational levels. For example, the need for creating a new system of records normally originates at the program level, where the records will be maintained and used. Data processing people may be involved in automating the system, and security personnel may assist in developing appropriate safeguards. The General Counsel offices at both components and headquarters levels review notices and reports of new systems for legal sufficiency.

Improved Directives Are Needed to Communicate Privacy Act Responsibilities

The Privacy Act and OMB publications do not provide detailed guidance on how agencies are to implement their Privacy Act responsibilities. Given the highly dispersed nature of Privacy Act functions, we examined how the 14 agencies communicated policies and assigned Privacy Act responsibilities throughout their organizations. We found that (1) three agencies had not issued comprehensive directives to assign responsibilities, (2) nine agencies issued directives but did not assign responsibilities consistent with the Privacy Act officers' position descriptions, and (3) eight agencies' directives did not address one or more significant responsibilities. In our opinion, improvements are necessary to assign responsibilities as well as to establish accountability for adhering to Privacy Act requirements.

Agencies have prepared Privacy Act regulations and, in some cases, directives. Agency regulations, published in the Code of Federal Regulations, generally serve to notify the public of procedures they may use to seek access to records. Directives, on the other hand, are internal documents aimed at setting the basic framework for Privacy Act operations.

Agency directives serve to communicate assignments of responsibility as well as establish accountability.

We analyzed the directives and Privacy Act officer position descriptions of the agencies to determine how they assigned responsibility for seven Privacy Act functions. As described in OMB Circular No. A-108 (now Circular No. A-130's app. I) these responsibilities include (1) allowing individuals access to their records, (2) establishing safeguards to prevent unauthorized disclosures, (3) establishing a program to periodically review recordkeeping policies and practices, (4) conducting training for individuals involved in maintaining systems of records, (5) publishing notices of systems of records, and (6) establishing and maintaining Privacy Act related procedures and directives. The seventh function is to report on and monitor agency participation in computer matching programs. Although not included in OMB's Circular No. A-108, this function was described in OMB's 1979 and 1982 computer matching guidelines and was incorporated into Circular No. A-130.

Three of the 14 agencies—Agriculture, Justice, and VA—have not issued comprehensive directives on Privacy Act implementation. We talked to officials at each agency to determine how agency policy is communicated and Privacy Act responsibilities assigned. Agriculture's Privacy Act officer said he holds periodic meetings with Privacy Act officers in components to discuss Privacy Act matters. He said that a departmentwide directive would be beneficial and plans to develop one. Justice's Assistant Director for General Services, the office that reviews system notices, said that each Justice component has a Privacy Act contact who works with the Justice person responsible for reviewing system notices. In addition, Justice annually reminds managers to report systems of records in accordance with OMB guidance and has developed an order on the Privacy Act security regulations for systems of records. A member of VA's Privacy Act staff said that while VA does not have a comprehensive Privacy Act directive, some responsibilities are assigned in various VA documents. For example, VA had assigned responsibility for preparing reports of new systems in their policy manual to systems managers. However, both he and the VA Privacy Act officer said that a comprehensive Privacy Act directive is needed.

Of the 11 agencies with directives, 8 have not assigned either one or more Privacy Act functions in either a directive or the Privacy Act officers' position descriptions. For example, none of the eight assigned responsibility for monitoring computer matching programs from a Privacy Act standpoint. Two of the agencies—Commerce and HHS—have

not assigned responsibility for Privacy Act related training. Two of the agencies—Education and Labor—have not assigned responsibility for evaluating Privacy Act implementation. Two of the agencies—HHS and HUD—have not assigned responsibility for developing and updating agency Privacy Act directives. Defense, Energy, and Interior were the only agencies which had assigned all of the seven Privacy Act functions in either their directive or the position description of the agency Privacy Act officer.

Nine of 11 agencies' directives did not accurately describe the roles and responsibilities of Privacy Act officers. For example, five agencies' directives did not show the Privacy Act officers' responsibility for evaluating implementation of the Privacy Act. Similarly, three directives did not show that the Privacy Act officer was responsible for training, and eight directives did not show the Privacy Act officers' responsibility for preparing and updating agency directives.

In our opinion, functions included in Privacy Act officers' position descriptions should be reflected in agency directives. While position descriptions describe the Privacy Act officers' responsibilities, they do not serve the same purposes as directives. Directives establish agency policy and procedures, identify the organizational location of Privacy Act responsibilities, and serve to inform all agency personnel as to appropriate offices or officials to contact when questions arise.

Complete agency directives would also benefit components. Of 37 selected components at six agencies where we conducted detailed analyses, 18 did not have their own directives and, consequently, relied on agency directives to communicate responsibilities. Of the 19 components that had directives, 17 did not address computer matching, 14 did not address evaluations, and 10 did not address training.

Role of Departmental Privacy Act Officer Needs to Be Reexamined

Each agency in our review except Justice and Labor[1] had established a position of agency Privacy Act officer to coordinate and oversee Privacy Act implementation. Our analysis of the position descriptions, activities, and resources allocated, however, indicate that these officials may not be providing oversight to the degree needed.

A Privacy Protection Study Commission was created by the Privacy Act of 1974 to investigate the personal data recordkeeping practices of governmental and private organizations. The commission concluded that a critical element to successfully implementing the Privacy Act was the designation of a single official with authority to oversee the implementation of the act. Following the commission's 1977 report to the President, a Cabinet-level coordinating committee was established to analyze commission findings. The coordinating committee agreed with the commission that it was desirable for agencies to have a single person responsible for overseeing Privacy Act implementation and cited four advantages: (1) increasing the visibility and awareness of Privacy Act responsibilities; (2) facilitating communication on Privacy Act matters; (3) enhancing consistent policy implementation; and (4) assisting in training and effective implementation of the act. The committee's effort became the Presidential Privacy Initiative.

As a result of the Presidential Privacy Initiative, OMB sent a memo to all agency heads in 1979 suggesting they designate an official with oversight responsibility for Privacy Act implementation. Each of the agencies has designated such an official and has delegated day-to-day responsibilities to a Privacy Act officer.

We reviewed the roles and responsibilities of Privacy Act officers and found that these individuals were not always assigned key functions. Table 2.1 summarizes the number of agencies that assigned seven selected responsibilities to Privacy Act officers in agency directives or position descriptions.

[1] Justice has not designated a Privacy Act officer but has assigned departmentwide responsibilities for reviewing system notices and preparing OMB's annual report submission. For purposes of this report we considered this individual to be the agency Privacy Act officer. Although Labor has not designated a Privacy Act officer, its directive assigns overall Privacy Act implementation responsibilities to the Solicitor and we have considered this individual to be the Privacy Act officer. As of May 28, 1986, this position was vacant.

Table 2.1: Functions Assigned to Privacy Act Officers by 14 Agencies

	Assigned to Privacy Act officers	Not Assigned to Privacy Act officers
Training	7	7
Computer Matching	1	13
Compliance evaluations	7	7
Safeguards	2	12
Systems Notices	6	8
Directives	12	2
Access	4	10

The table shows that significant functions were not assigned to agency Privacy Act officers. For example, although computer matching is one of the more controversial activities having Privacy Act considerations, 13 of the 14 agencies had not specifically assigned any role to the Privacy Act officer. Because Privacy Act activities are dispersed and conducted throughout agencies and their many components, we believe the Privacy Act officers should have some coordinating role in each of these critical functions. As discussed in the following chapter, our detailed review of selected Privacy Act functions at six agencies showed that Privacy Act officers were not always actively involved in all of these areas and Privacy Act and OMB guidance was not always followed.

Even if the roles and responsibilities assigned to Privacy Act officers were expanded, it is doubtful whether under current circumstances they would be able to meet them given the resources provided to them. Table 2.2 lists the resources and locations of agency Privacy Act officers and their staffs as of May 1986.

Table 2.2: Location and Resources of Agency Privacy Act Officers and Staff

Agency	Senior official	Immediate office	Grade of Privacy Act officer	Estimated staff years (Officer/ staff)[a]
Agriculture	Assistant Secretary, Office of Governmental and Public Affairs	Special Programs Division	12	.25/0
Commerce	Assistant Secretary for Administration	Information Management Division	15	.05/.40(1)
Defense	Assistant Secretary of Defense (Comptroller)	Defense Privacy Board	SES	.90/1.80(2)
Education	Deputy Under Secretary for Planning, Budget and Evaluation	News and Information Division	12	.20/.60(1)
Energy	Assistant Secretary for Management and Administration	Freedom of Information and Privacy Acts Branch	14	.40/.30(4)
Health and Human Services	Assistant Secretary for Public Affairs	Freedom of Information/ Privacy Division	14	1/.60(2)
Housing and Urban Development	Assistant Secretary for Administration	Information Policies and Management Division	14	.50/0
Interior	Assistant Secretary for Policy, Budget, and Administration	Division of Directives and Regulatory Management	14	.30/0
Justice	Assistant Attorney General for Administration	Mail, Fleet, and Records Management Services	12	1/0
Labor[b]	Solicitor	Solicitor	—	—/.55(6)
State	Assistant Secretary for Administration	Information Access and Services Division	15	.25/4.85(12)
Transportation	Assistant Secretary for Administration	Information Requirements Division	14	.05/0
Treasury	Assistant Secretary for Management	Disclosure Branch	13	.33/.97(1)
Veterans Administration	Associate Deputy Administrator for Management	Paperwork Management and Regulations Service	15	.03/.47(3)

[a]The number in parentheses designates the number of staff available to assist the Privacy Act officers.

[b]Grade of the Solicitor and estimated time devoted to Privacy Act matters were not available due to the position's vacancy.

Except for DOD and Labor, Privacy Act officers were mid-level managers whose grade levels ranged from GS-12 to GS-15. They were often two layers removed from the senior agency official who directed the organization to which they were assigned. Generally, the senior official was an Assistant Secretary with many responsibilities other than Privacy Act implementation.

Privacy Act officers also had limited resources to perform their Privacy Act duties. By their own estimates, 10 of the 14 Privacy Act officers spent less than half their time on privacy matters; two were full time. Five had no staff. Nine had staff but for seven of these officers, their staffs spent less than one full staff year on Privacy Act matters.

Except for HHS and Justice, all Privacy Act officers had other duties that competed for their time and resources. Nine of the 14 Privacy Act officers were responsible for some aspect of the agency's implementation of the Freedom of Information Act. For example, Energy's Privacy Act officer was Chief of the Freedom of Information/Privacy Act Branch; he spent about 40 percent of his time on Privacy Act issues. Others, such as the VA Privacy Act officer, who spent 3 percent of his time on the Privacy Act, was the agency's focal point for records management, forms management, mail management, and travel management. Transportation's Privacy Act officer's primary responsibility was implementing the Paperwork Reduction Act which he estimated took 90 percent of his time.

Agency component and other organizational units may also designate individuals to coordinate and/or oversee Privacy Act activities. Each of the 37 components of the six agencies reviewed in detail identified such an individual. Our analysis showed that, like agency Privacy Act officers, these individuals generally held mid-level management positions and worked on Privacy Act matters on a part-time basis. Because the individuals held different positions and titles, we have referred to them as component Privacy Act officers. A table summarizing this analysis is in appendix II.

Like their counterparts at the agency level, component Privacy Act officers were generally mid-level managers at grades GS-12 to GS-15. However, their grade levels ranged from a GS-8 secretary at Interior's Aircraft Services to Senior Executive Service positions at six components.

Of the 37 component Privacy Act officers, 22 spent 10 percent or less of their time on Privacy Act functions. Only at the Health Care Financing Administration in HHS was the Privacy Act officer a full-time position. Although 29 of the 37 Privacy Act officers had additional staff resources, in 28 components the staff spent less than 1 full staff year on Privacy Act matters. These estimates do not include other component employees who may become involved in Privacy Act matters such as handling access and disclosure requests.

As the staff years suggest, all component Privacy Act officers, except the Health Care Financing Administration, had other duties. For example, the Bureau of Mines' Privacy Act officer was responsible for personal property management, space management, motor vehicle management, and energy conservation. Treasury's Bureau of the Public

Debt's Privacy Act officer served as an advisor for the Bureau's marketable securities programs. Also, like their agency counterparts, 21 Privacy Act officers had some responsibility for implementing the Freedom of Information Act.

Privacy Issues Not Covered by the Act

Agencies may engage in activities that have privacy implications outside the context of the Privacy Act of 1974. For example, taping of conversations, workplace monitoring, polygraphs, fraud hotlines, and computer profiling may have personal privacy implications but because they may not involve Privacy Act systems of records, would not be subject to the act.

We asked agency Privacy Act officers whether there was a focal point or central mechanism to identify and deal with non-Privacy Act privacy issues raised by these activities. We were interested in determining whether attention was being given to such things as

- assessing the impact of the activities on personal privacy,
- determining whether activities with privacy implications should be undertaken,
- determining who should be involved in the activities (personnel/component), and
- providing appropriate controls for management oversight.

The Privacy Act officers at 10 of the agencies told us there was no central focal point to address privacy issues not covered by the act. Four of the 10 Privacy Act officers said they could be minimally involved in such issues but only when asked. Five said they were not involved at all with these issues. DOD's Privacy Act officer said that, while he did not consider his office to be a central focal point, his office would become involved in most of the privacy-related concerns dealing with such issues.

The remaining four Privacy Act officers believed there was a focal point. The State and Labor Privacy Act officers said they acted as the focal point. In addition, the Privacy Act officer at Energy believed that a focal point existed in Energy's defense programs area. The Privacy Act officer at Transportation said that the Office of Security would serve as a focal point.

We asked the Privacy Act officers for their views on the desirability of having a central focal point to address privacy issues not covered by the

act. Seven believed that a focal point to address some or all of the issues would be beneficial, while two expressed doubts about its need or practicality. The remaining five Privacy Act officers did not express an opinion.

The limited involvement of Privacy Act officers and the absence of a centralized mechanism to identify and address activities having privacy implications not subject to the Privacy Act does not imply that these privacy issues are not addressed. Such activities may occur virtually anywhere within an organization and may be addressed as they arise. However, in our opinion, it might be worthwhile for agencies to take steps to channel information concerning such activities to the Privacy Act officer or other centrally located official. This individual would be in a position through daily contacts on privacy matters to share information throughout the organization and thereby heighten awareness of privacy implications.

Experiences of Six Agencies Show Improvements Are Needed

We examined in depth how six agencies—HHS, Interior, Justice, Labor, Treasury, and VA—were complying with selected provisions of the Privacy Act and OMB guidelines pertaining to (1) assuring adequate safeguards of newly created and modified systems of records, (2) automating systems of records, (3) computer matching, (4) Privacy Act training, and (5) internal evaluations. We found that the agencies need to make improvements in each area.

- While OMB suggests that agencies should conduct detailed risk assessments for newly created or modified systems of records to assure their security and confidentiality, the agencies were able to provide evidence of such an assessment for only 1 of the 27 systems of records that were established or modified in 1983. Agency Privacy Act officers told us they rely on component organizations to conduct the risk assessments; however, component officials said this function was not always performed.
- Systems of records that become automated are considered to be new systems subject to the OMB guidelines if the automation results in greater access to the records. None of the three agencies that automated systems during the period of our review followed OMB's guidelines.
- Agencies have not reported accurate data to OMB on the extent of their computer matching programs. Two organizations considered their matching programs to be exempted from OMB guidelines, although OMB's concurrence was not sought. Our analysis of 26 computer matching programs showed that 6 did not follow OMB guidance.
- The training needs of individuals involved with Privacy Act activities were not assessed or provided in a systematic manner. Privacy Act officials at four components told us they do not provide Privacy Act training. In the remaining 33 components, Privacy Act officers said some training is received although not all Privacy Act officers maintained data on who attended.
- Agencies do not routinely conduct internal evaluations of Privacy Act operations which would provide senior agency officials with feedback on the effectiveness of the operations or on areas needing improvement.

Detailed Risk Assessments Were Not Conducted or Were Not Available for New and Revised Systems of Records

To establish or change Privacy Act systems of records, the act requires agencies to publish notices in the Federal Register listing a number of descriptive elements. The act also requires agencies, through reports on new systems, to provide adequate advance notice to the Congress and OMB of any proposal to establish a new system of records or, under certain conditions, alter an existing system.

Safeguarding personal information is vital to complying with the Privacy Act. The act requires agencies to establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records. To accomplish this, OMB's guidance calls for a brief description of the steps taken to minimize the risk of unauthorized access to the system to be included in the agency's submission at the time the system is established or revised. In addition, OMB's guidance to agencies calls for a more detailed assessment of the risks and specific administrative, technical, procedural, and physical safeguards established to be available on request.

During 1983, the Departments of HHS, Interior, Justice, Treasury, and the VA published notices and prepared reports on 27 new or revised systems of records. The Department of Labor did not have new or revised systems in 1983. The Privacy Act officers at the five agencies said they reviewed draft notices and reports to assure that required data elements were included and properly stated. But they said they did not monitor compliance with the requirement that detailed assessments of the risks and safeguards established be conducted and available on request. Consequently, they had no available information on the extent to which their agencies followed the OMB guidance.

For each of the 27 new or revised systems, we requested a copy of the detailed risk assessment. Of the five agencies, HHS was able to provide a risk assessment for one of its systems.

- The VA Privacy Act officer said that components are responsible for conducting detailed risk assessments. A member of the Privacy Act officer's staff in the component responsible for the one new system instituted in 1983 said he did not know if a detailed risk assessment was conducted. Because of our inquiry, the staff member contacted a program official and was assured that the potential risks and necessary safeguards were addressed at the time the system was proposed.
- Treasury's Privacy Act officer said she did not have copies of risk assessments for the one new system and two revised systems instituted in 1983. The components responsible for the systems were unable to

provide any risk assessments. The Privacy Act officer said she had reviewed system specifications for other systems in the past when her review of their proposed notices or reports raised questions.

- Interior's Privacy Act officer said that the bureaus are required to perform risk assessments. However, when we asked the components for copies of the risk assessments for the three new and revised systems for 1983, one component responsible for two systems responded that risk assessments were not conducted. Another component responsible for the third system of records said that, as far as it could determine, no formal risk analysis had been performed. In addition, this component said that its impression is that the requirement has generally been ignored.
- Justice instituted 10 new or revised systems in 1983. Justice's official responsible for reviewing system notices said that she did not ask for copies of detailed risk assessments because she believed it was not her responsibility. Our follow-up work at the appropriate Justice components revealed that risk assessments were not available. Justice officials said they believed that the risks of unauthorized access were considered, although the review process was not put in writing. They also said that in 1985 Justice awarded a contract to study security needs at its two data centers.
- One of the five HHS components we visited (the Office of General Counsel) had performed a risk assessment; the remaining four components of HHS did not perform risk assessments for nine new and revised systems instituted in 1983. The Chief of the SSA Privacy Branch said he did not request risk assessments because he was relying on the originating component to contact appropriate system security personnel as called for in the SSA directive. The Public Health Service's Privacy Act officer said she never asked for detailed risk assessments during her review of notices and reports but she had assumed they were done. According to this official, she included a question dealing with risk assessments in an internal control review and found that risk assessments were not being done. The person who was the Health Care Financing Administration's Privacy Act officer during 1983 said she was not familiar with the term risk assessment except in reference to computer security and did not remember risk assessments being included in HHS' checklist for creating new systems of records. Although the checklist points out that the measures taken to minimize the risk of unauthorized access to the system should be described in systems reports, it does not state a requirement for detailed risk assessments. An official from the Office of Inspector General said she was not certain whether a risk assessment was conducted. She suggested that it may have been done, but not incorporated into a single document and

retained. She said the subject system of records was temporary and was deleted after approximately 6 months.

Several agency officials raised the question of whether risk assessments need to be kept on file in the years after the system of records was created and whether the assessment needs to be incorporated into a single document. OMB's December 1985 Circular No. A-130, Management of Federal Information Resources, shows that it would be beneficial for agencies to keep risk assessments on file regardless of whether they are incorporated into a single document.

Appendix III to the circular, "Security of Federal Automated Information Systems," establishes controls to be included in federal automated systems security programs where sensitive records, including Privacy Act records, are used. In part, this appendix is in response to prior GAO work on the implementation of the Federal Managers Financial Integrity Act which reported that (1) agencies have identified material weaknesses in automated data processing, including system security, and (2) agencies could better evaluate automatic data processing controls with additional OMB guidance. The appendix, among other things, instructs agencies to conduct periodic reviews of sensitive applications and to recertify security safeguards at least every 3 years. It states that the reviews should be considered part of the agencies' internal control reviews pursuant to the Financial Integrity Act. In our opinion, fulfillment of these instructions would be facilitated if agencies fully document risk assessments on their Privacy Act systems of records and keep them on file.

We discussed this with OMB. OMB's senior policy analyst for Privacy Act matters said he would consider amending Circular No. A-130 to instruct agencies, in submitting their reports on new or altered systems of records, to include information on where the formal risk assessment is located so that OMB could obtain a copy, if necessary.

Agency Automation of Systems of Records

OMB's guidance on automation of systems of records states that when such a change creates "the potential for either greater or easier access" agencies need to prepare a new system report and a revised system notice. At the same time and as part of the process, agencies are to conduct a detailed assessment of risks and safeguards. Three of the six agencies reported automating systems during 1983. We discussed how the OMB guidance was applied with Privacy Act officials at each of the three agencies.

- Interior reported that 44 systems of records were automated during 1983. According to the agency Privacy Act officer, the bureaus are responsible for adhering to OMB's guidelines. We discussed the system automations at two bureaus which accounted for 23 of the systems. The privacy coordinator at one bureau which automated 11 systems said bureau personnel did not review the 1983 automations until 1984 and 1985. At that time they concluded that the automations did not meet OMB's criteria of creating greater or easier access because they did not increase the number of personnel who had access to the records. According to this official, the automations entailed upgrading equipment, and only those who had access to the earlier systems continued to have access. The privacy coordinator at the second bureau, which automated 12 systems, said he did not know if the question of whether OMB's guidance was applicable to the automation actions had been addressed. Our analysis of the system notices for these 12 systems showed that they were updated in 1983 to reflect some changes, but the sections related to automation were unchanged from their last republication in 1977. One system was still described as a manual system.
- Justice automated five systems of records during 1983 and prepared reports on new systems and revised system notices for each. Because of personnel changes, we were able to talk to personnel knowledgeable about only three of the systems. The Privacy Act coordinator of the component responsible for two of the automations said that he assumed that all automations should result in a report and new system notice. A staff member in another component responsible for a third automation believed the automation met OMB's greater access criteria because information would be input at remote terminals. Although both said that OMB's publication guidance was followed, neither individual believed that risk assessments were conducted. One of the individuals told us she was unaware that the assessments were needed. The second individual recalled that his predecessor discussed Justice's security requirements with the system manager but did not discuss OMB's risk assessment provision.
- Labor automated two systems. According to the Privacy Act staff, the responsibility for determining whether a new system report and revised notice are necessary rests with components. Officials at the component involved were unaware of OMB's guidance on automated systems and acknowledged that the system notices published in the Federal Register still categorize the two systems as being manual. These officials and a staff member of the Labor Privacy Act officer said they would review OMB's instructions and issue the necessary publications for these systems.

In its December 1985 publication of the President's Annual Report on the Agencies' Implementation of the Privacy Act of 1974 for calendar years 1982 and 1983, OMB identified the effects of automation as an area of concern for future study. OMB observed that 80 percent of all systems were manual when the Privacy Act was drafted and that there has been a continuing trend towards automation, including an estimated 500,000 microcomputers in use by 1990.

If OMB conducts an automation study, we believe it should include how agencies implement its guidance pertaining to automated systems. On December 12, 1985, OMB changed its criteria on the automation of existing systems from those that create "the potential for either greater or easier access" to those that create "substantially greater access . . . ." In our opinion, both of these descriptions lack specificity and may be subject to wide interpretations. This is particularly true in view of the fact that decisions may be made by many different personnel who are responsible for Privacy Act systems of records.

Improvements Can Be Made in Overseeing Computer Matching

Computer matching—the comparison of two or more sets of computerized systems of records to identify individuals who are included in more than one—is an activity that raises privacy concerns. To provide guidance and oversight of agency matching programs, OMB issued detailed matching guidelines in 1979 and revised them in 1982.

Each of the six agencies in our detailed review participated in computer matching programs in 1983. We found that the number of programs agencies reported to OMB understated the actual amount of reportable matching activity. Several of the agencies used varying criteria in reporting their matching programs to OMB, and others' recordkeeping practices were poor. In some cases, agency Privacy Act officers believed that more specific routine uses were needed for releasing information; however, the information was released before the disclosures came to their attention. Also, one agency disclosed information for a matching program without a written agreement on how the information would be used and conducted two programs without publishing notices in the Federal Register.

Computer Matching and OMB's Guidelines

In conducting a matching program, two computer files are run against each other with a software package that instructs the computer to search for certain personally identifiable variables, for example, identical social security numbers, names, or addresses. When the program

identifies duplicate information (or information that is similar to a predetermined degree), such data are considered "raw hits" that need to be refined and verified. Matching is used for such purposes as detecting unreported income, duplicate benefits, overpayments, and ineligible recipients.

A matching program by the former Department of Health, Education, and Welfare in 1977, called "Project Match," is commonly cited as the federal government's first major computer matching effort. It involved comparing the computer tapes of welfare rolls and federal payroll files in 18 states, New York City, and Washington, D.C. The goal was to detect federal employees who were fraudulently receiving benefits through the Aid to Families with Dependent Children program.

The constitutional and statutory legitimacy of computer matching has been questioned by a number of privacy advocates, most notably the American Civil Liberties Union which was primarily concerned about the impact of computer matching on individual rights. Their concern stems from the fact that a computer matching program is usually not directed at an individual—but rather at an entire category of persons—and not because any one of them is suspected of misconduct but because the category is of interest to the government. Privacy advocates are concerned that such programs—which they view as generalized "fishing expeditions"—may violate the Fourth Amendment right to be free from unreasonable searches and seizures.

Opponents of computer matching also question its statutory authority. The Privacy Act restricts disclosure by federal agencies of personally identifiable information, unless the record subject consents or unless the records fall under one of 12 exceptions. One major exception to this rule involves the "routine use" provision, defined as the use of a record for a purpose which is compatible with the purpose for which the record was collected. Since administration of the Privacy Act is left almost entirely to the agencies it regulates, some agencies have developed broad routine use justifications for matching of personal records. The opponents of matching argue that these broad routine use justifications circumvent the underlying privacy principle that individuals should be able to exercise control over information about themselves which they provide to the government.

Proponents of computer matching believe that the routine use compatibility requirement should extend to disclosures that agencies perceive as

necessary, proper, and of benefit to the government. They feel that carefully managed computer matching is a valid internal control technique. Further, the Congress has authorized the use of computer matching in various programmatic areas specified in several statutes, such as the Deficit Reduction Act of 1984.

Under its Privacy Act oversight authority, OMB in March 1979 issued matching guidelines "to aid agencies in balancing the government's need to maintain the integrity of Federal programs with the need to protect an individual's right to privacy." In May 1982, OMB revised its earlier guidance, clarifying parts and simplifying others.

Matching programs covered by the guidelines entail a source agency and a matching agency. Source agencies disclose personal data to be used by the matching agency in performing the program. The guidelines specify that, before disclosing personal data, source agencies are to require the matching agencies to agree in writing that the data will not be used to extract information concerning "non-hit" individuals for any purpose. Matching agencies, according to the guidelines, are to publish a notice in the Federal Register, describing the matching program, and are to send copies of the notice to OMB and the Congress concurrently.

The guidelines specify that certain types of matching programs are not covered by the provisions. Examples are

- those which do not compare a substantial number of records,
- checks on specific individuals to verify data in applications for benefits done reasonably soon after the applications are received, and
- programs done by an agency using its own records.

More Complete Data Needed on the Extent of Computer Matching

Congressional hearings and various studies have documented that no accurate accounting exists on the number of computer matching programs being conducted by federal agencies. We compared calendar year 1983 computer matching statistics reported to OMB by the six agencies with data we obtained at the agencies. We also obtained information that agencies provided to the Office of Technology Assessment (OTA) for its recent study of federal information technology.[1] We found that the agencies used varying criteria in reporting matching programs to OMB. We also found discrepancies caused by poor recordkeeping. Overall, the

[1]Federal Government Information Technology: Electronic Record Systems and Individual Privacy, June 1986, OTA-CIT-296.

agencies participated in more matching programs than they reported to OMB and the Congress.

For the preparation of the President's annual report to the Congress on Privacy Act implementation, OMB asks agencies to annually report the number of matching programs in which they participated as a source agency and as a matching agency. Table 3.1 shows the number of 1983 programs the six agencies we reviewed reported to OMB and the number of programs that we were able to identify. In many instances the programs were conducted among two or more of the six agencies we reviewed; thus, adding the columns would overstate the total numbers.

Table 3.1: 1983 Computer Matching Programs at Six Agencies

	Number of programs reported to OMB	Number of programs GAO identified
Health and Human Services	5	19
Interior	2	2
Justice	1	2
Labor	13	15[a]
Treasury	1	5[b]
Veterans Administration	21	19[c]

[a]Our reconciliation of Labor's programs showed that because of administrative error, Labor reported five programs that did not occur. It also conducted seven programs which it did not report to OMB. Labor believes that three of these programs were not subject to OMB's guidelines. We include them because in two cases, participant agencies reported them to OMB, and in the third case, the available documentation describes a program that we believe should also be reported to OMB.

[b]Includes four matching activities involving IRS that IRS believes may not be matching programs as defined by OMB guidelines. We include them because the four participant agencies agreed with us that the programs are covered by the guidelines.

[c]We found that VA conducted two programs that it did not report to OMB. In addition, it reported four activities which it misidentified as matching programs.

Discrepancies Caused by Agencies' Interpretations of OMB Matching Guidelines

Most unreported matches were due to agencies' interpretations of the OMB guidelines. Two agencies—the Internal Revenue Service and HHS' Office of Child Support Enforcement (OCSE)—believed that their matching programs were not subject to OMB's guidelines. Labor believed that three of its programs were not subject to the guidelines. Other agencies differed in how they reported matching programs that were performed periodically and extended over more than 1 year.

During the course of our review four agencies—the Bureau of Prisons, SSA, OCSE, and Labor—indicated that they participated with IRS in computer matching programs. In addition, IRS provided information to the OTA stating IRS' participation in seven other matching programs during 1983. An IRS official told us that information on computer matching activities is not reported to OMB because IRS was exempt from the guidelines. The official also said that data reported to OTA, and possibly by the four agencies, may be in error because this may have included computer activities that were not matching programs as defined by the OMB guidelines. He said that IRS does not maintain readily available records that show how many matching programs it actually participated in because of its exemption. The official said that IRS would have to examine many computer operations to determine if they were matching programs as defined by OMB's guidelines.

According to Treasury's Privacy Act officer, Treasury requested and received OMB's approval to exempt IRS' tax administration matching programs from adherence to the 1979 matching guidelines. The official explained that Treasury received assurance from OMB that the 1979 guidelines were not intended to apply to tax administration matching programs but rather to anti-fraud programs related to federal assistance type payments, such as VA or other federal loans. Treasury also believed that section 6103 of the Internal Revenue Code provided sufficient safeguards for personal data and that compliance with the guidelines would cause an unnecessary administrative burden. Treasury continued to apply this exemption after OMB issued its revised guidelines.

We discussed Treasury's belief that IRS is exempt from OMB's 1982 guidelines with OMB's senior policy analyst for Privacy Act matters. This official said that, unlike the 1979 guidelines, OMB's 1982 guidelines do not distinguish anti-fraud matching programs from other types, and consequently IRS needs to adhere to the 1982 provisions. On March 20, 1986, OMB communicated its position to Treasury that IRS should follow the guidelines. As of April 28, 1986, IRS had not responded to OMB's position; although according to an Office of General Counsel attorney, Treasury continues to believe IRS is exempt.

OCSE did not report at least two recurring 1983 matching programs in which it participated. OCSE, with its parent locator service, was the source agency in programs with VA and IRS to identify the addresses of missing parents. In addition to VA and IRS, OCSE participates in such matching programs with DOD, the Selective Service System, and the

National Personnel Records Center. These programs are generally conducted monthly, except for IRS' weekly operation. An OCSE official told us the agency's matching programs were not reported to OMB because OCSE believed OMB's guidelines did not apply. According to this official, OCSE considered itself a "conduit" for this matching activity—receiving data on absent parents from states, transmitting it to agencies for matching, receiving the results, and forwarding them to the states. OCSE did not consult with HHS' Privacy Act staff or OMB about this determination. After our discussions, the official agreed that OCSE is subject to the guidelines and stated that future matching programs will be conducted in accordance with the guidelines and will be reported to OMB.

Labor participated in three matching programs in 1983 that it did not report to OMB. All three involved the Employment Standards Administration. It was source agency for (1) a one-time program with the National Aeronautics and Space Administration (NASA) dealing with hearing loss claims at a NASA research center and (2) a program performed periodically with Interior to ensure that Labor charges Interior for only Interior employees' workers' compensation payments. In the third program, Labor was matching agency with the United Mine Workers Health and Retirement Funds as source.

Labor's Privacy Act staff, using a similar rationale for the two source agency programs, determined that neither was subject to OMB's matching guidelines. The reason given was that the computer tapes sent to NASA and Interior contained information on only those agencies' employees. Labor thus believed that both programs were, in effect, internal to the two agencies and not subject to the guidelines. NASA and Interior, on the other hand, published Federal Register notices for the matching programs. The respective notices showed that these agencies considered the programs to be subject to OMB's guidelines. Because the different interpretations by Labor and the two other agencies create inconsistent reporting, we discussed them with OMB's senior policy analyst for Privacy Act matters. This official said that the match with NASA was subject to OMB's guidelines and should have been reported by Labor. He said he would have to further review Labor's program with Interior to determine if it is subject to the guidelines.

The third matching program that Labor did not report to OMB is a recurring one that was created to assist the United Mine Workers Health and Retirement Funds in determining the eligibility for black lung benefits of that agency's beneficiaries. Where proper eligibility is determined, the program further assists in identifying the associated mine operators

who may be responsible for reimbursing the source agency. Labor's Privacy Act staff said they view the program as essentially a billing procedure whereby the allocation of benefit payments is determined. OMB, however, does not include programs such as this one as exceptions to its guidelines. Thus, we believe Labor should have reported the program to OMB and, since the program is ongoing, should continue to do so.

Inconsistent reporting to OMB on the number of matching programs agencies conducted also occurred because of the manner in which agencies treated programs that were initiated before 1983 but continued on a periodic basis, including the 1983 time frame. Interior, in responding to OMB's request for the number of matching programs participated in during 1983, included one that was initiated in 1982. This program is a recurring one, and because it was continued into 1983, Interior believed it should be included in the 1983 data submission to OMB. VA also followed this practice and included its participation in three programs that were initiated in earlier years. HHS' Social Security Administration and Office of the Assistant Secretary for Personnel, in contrast, did not report their 1983 participation in 12 programs that were initiated in prior years.

Unless participation in all matching programs is reported, extensive matching activities may occur but will not be reflected in the report to the Congress.

Discrepancies Caused by Poor Recordkeeping

Other matching programs were incorrectly reported because of inaccurate and incomplete recordkeeping.

Labor did not report four matching programs to OMB involving the black lung program, which is in the Division of Coal Mine Workers Compensation. The Privacy Act coordinator for the Employment Standards Administration (which contains this division) said the computer matching paperwork did not go through his office. Following our inquiry, a workers compensation specialist in the division was assigned to locate documentation of the black lung matching programs. He was able to find very little matching-related paperwork until we described for him the data that Labor had provided for OTA's recent federal information technology study.

Labor's Employment Standards Administration reported that it conducted five matching programs involving the Federal Employees Compensation Act area in 1983. However, we found that the Administration

did not perform any programs for this area in 1983. The Privacy Act coordinator said he may have been confused about how to fill out the OMB data request; the program office had served as the source agency for five matching programs, and he entered those correctly.

The Administration's Privacy Act coordinator has initiated procedures to ensure that matching activities are properly reported in the future. The procedures require all components of the Administration, when proposing participation in a match, to contact the Privacy Act coordinator regarding the documentation and any OMB clearance that may be necessary. Further, the Privacy Act coordinator must concur in all computer matching documentation.

VA's Department of Veterans Benefits reported four activities as source matching programs that were instead external releases of information for purposes other than computer matching. This department also did not report a one-time matching program that it conducted. Another program not reported by VA involved the Office of Budget and Finance as a source. A member of the central office Privacy Act staff said an administrative error caused the program not to be reported to OMB. Because of our findings, the central office staff instituted computer matching reporting procedures that require VA components to submit specific details on all of their matching programs to the central office.

Finally, two unreported source agency programs occurred at Treasury and Justice. One involved Treasury's Office of Inspector General, which is organizationally within the Office of the Secretary. Labor was the matching agency. Treasury's Privacy Act officer said that since she is also located within the Office of the Secretary, she did not query components of that office about their matching activities since all matches would normally be reported to her before being conducted. The second matching program involved Justice's Bureau of Prisons as a source agency to IRS. According to the bureau Privacy Act officer, his records did not include this match; otherwise he would have reported it.

Problems Noted Involving Specific Matching Activities

We reviewed 26 matching programs that were subject to OMB's 1982 guidelines[2] and found that three agencies did not follow the guidelines' provisions in 6 of the programs. For three of the programs, agency Privacy Act officers believed that more specific routine uses were needed

[2]The six agencies were involved in 35 matching programs; 9 of these were subject to the 1979 guidelines. These earlier guidelines contained different provisions from the 1982 version, especially

for releasing information; however, the information was released before the disclosures came to their attention. In one program, the source agency did not obtain a written agreement from the matching agency on how the data would be used, although it did obtain oral agreement. Finally, in two other matching programs, an agency did not publish Federal Register notices. We also found one instance where an agency disclosed records to a nonfederal entity but, because OMB guidance is silent on such matching programs, did not publish a Federal Register notice.

Disclosures Under Routine Use Provisions

The OMB guidelines instruct agencies serving as source agencies in matching programs to ensure that disclosures are in accord with the Privacy Act. The act, with 12 specific exceptions, disallows the disclosure of records without the record subject's consent. One exception, called the routine use provision, allows the disclosure if the records will be used in a manner that is compatible with the purpose for which they were originally collected. The routine uses must be published as part of the public notice provided for the entire system of records.

For the 26 matching programs conducted in 1983, we found that five of the six agencies participated as source agencies and made disclosures under the routine use provision on 17 occasions. Our analysis showed that generally the published routine uses were consistent with the purposes of the programs. However, in three instances, Privacy Act officers believed that sufficiently descriptive routine uses were not present in the system notices. According to the Privacy Act officers, the disclosures occurred before the matter came to their attention.

Both Treasury's Office of Inspector General and IRS were identified as source agencies for matches conducted by the Department of Labor. Labor performed the program to identify individuals who received unemployment insurance compensation during periods of federal employment. It matched the employee payroll records of seven federal agencies with the unemployment insurance claimant records of 14 state employment security agencies. Treasury and IRS released to Labor certain employee payroll data that they extracted from their payroll record systems. Treasury's Privacy Act officer told us that new routine uses more closely associated with the intended program should have been published before releasing the data. She said she could not recall being aware of the disclosures until after they occurred. She said routine uses

regarding public notice; Federal Register publication was called for only in the 1982 guidelines. Consequently, we reviewed the 26 programs for compliance.

allowing such disclosures would be prepared and published in the Federal Register.

Interior was also a source agency in Labor's unemployment compensation matching program. At the request of Interior's Inspector General, several components extracted data from multiple payroll systems for release to Labor. Interior's Privacy Act officer and an attorney in the Office of the Solicitor said that the issue of routine uses for the matching program was not addressed until after the disclosures were made. The attorney later reviewed the routine uses for each of the systems and determined that one use was present in each of the notices that was sufficiently broad to permit the disclosures. However, Interior's Privacy Act officer and a second attorney in the Solicitor's office believed that the cited routine uses in the system notices did not precisely describe the computer matching process to be used in the intended disclosures. Therefore, after the disclosure for the matching program, Interior published a specific new computer matching routine use for each of the payroll systems.

Source Agency Agreements

Under the OMB guidelines, federal source agencies are responsible for obtaining written agreements from the matching agencies that specify the conditions governing the use of the matching files. The agreement is to make explicit the conditions under which disclosure will be made and is aimed at, among other things, assuring that the disclosed information will be used only for the intended purposes. Because the six agencies served as source agencies in 17 of the 26 matching programs, source agency agreements should have been obtained. We found with one exception that the agencies had them on file.

The one exception involved the VA which disclosed records to the Georgia Bureau of Employment Security as part of its program to match state wage records to identify any unwarranted payments of VA pension and certain compensation benefits caused by beneficiaries' underreporting or failing to report earned income. VA's Office of Inspector General conceived and coordinated the program and published the matching notice in the Federal Register. The state agency, however, did not want to release its entire file, so VA provided its data and the state agency performed the initial matching procedure. Although VA obtained no written agreement, the Inspector General's Privacy Act staff said that Georgia officials orally agreed to the conditions outlined in the OMB guidelines and returned the computer tape to VA when the program was

completed. The program staff said they overlooked obtaining a written agreement.

Federal Register Notices

A responsibility assigned to matching agencies by the OMB guidelines is the publication in the Federal Register of a notice describing the matching program. The notice, to be published "as close to the initiation of the matching program as possible," is to include such elements as a description of the personal records to be matched and the safeguards to be used for protecting this data.

The six agencies we reviewed served as the matching agency in 14 of the 26 matching programs. We found two instances where an agency did not provide notice in the Federal Register. The notices were not published because of an apparent misunderstanding as to which agency had this responsibility. The two programs involved OCSE and Army serving as source agencies to VA's Department of Veterans Benefits. Both programs were conceived by and conducted for the benefit of the source agencies. The component's Privacy Act officer said staff involved in the programs told him the two source agencies had responsibility for matching notice publication since the programs were for their benefit. VA records, however, do not indicate that the issue of notice publication was discussed among the agencies sufficiently to ensure that agreement was reached on who had this responsibility. According to OMB's guidelines VA, as the matching agency, should have published the notices.

One additional matching program for which a notice was not published highlights a shortcoming in the OMB matching guidelines. Nonfederal organizations that use federal agency data in matching programs are not required to publish notices in the Federal Register. Thus, a notice was not published for a program using SSA data where the State of California was the matching agency. The OMB senior policy analyst for Privacy Act matters said the guidelines should be amended to provide that federal agencies publish notices when they participate as sources to nonfederal entities. This amendment could become even more significant in the future since the Deficit Reduction Act of 1984 requires, in effect, that federal/state matching activities be expanded.

OMB Computer Matching Checklist

In December 1983, OMB issued a computer matching "checklist" to assist agencies in adhering to OMB guidelines. Agencies are to complete the checklist and maintain it in their files. It contains several questions to be answered for each matching program in which agencies participate.

including whether and when (1) routine use provisions were published, (2) source agency agreements were obtained, and (3) a notice of the program was published.

While the checklist could help prevent the problems we found for matching programs conducted in 1983, the agencies need to ensure that all components use it for their programs. We contacted Privacy Act staff at the agencies' 15 components that participated in matching programs in 1983 and found that the staff in 10 components were aware of the checklist. At 6 of the 10 components the staff told us the checklist had been used for one or more programs; the other 4 said they had not participated in any programs since the checklist's issuance, but it will be used when programs occur. At the remaining five components, which were involved in 18 of the 35 programs conducted in 1983, the Privacy Act staff were not aware of the checklist's existence.

Agencies Need to Better Monitor Privacy Act Training

In Circular No. A-108, OMB made agency heads responsible for conducting training for all personnel who are in any way involved in maintaining Privacy Act records for the purposes of (1) apprising them of their Privacy Act responsibilities and (2) familiarizing them with agency procedures for implementing the Privacy Act. In a December 1985 revision, OMB strengthened its instructions and made agency heads responsible for annually reviewing agency training practices to ensure that all agency personnel are familiar with the act's requirements, agency implementing regulations, and any special requirements that their jobs entail.

Although Privacy Act training was offered, it was not always monitored by agency or component Privacy Act officers to track employees who receive or need it. Discussions with the agency Privacy Act officers and 37 components of the six agencies included in our review disclosed the following.

- Two of the six agency Privacy Act officers said they were not involved in training because of resource constraints. Another two officers have provided training, although one stated that resource limitations have prevented his involvement over the past several years. The remaining two Privacy Act officers said that the training function is delegated to other units.
- Thirty-three of the 37 components reported that Privacy Act training was provided and ranged from internal programs and discussion at management conferences to external training courses, although in some

instances attendance was optional. Fourteen Privacy Act coordinators said they do not maintain data on who attended.

- The remaining four components, at one agency, reported that they do not provide Privacy Act training.

For its 1985 presidential report, OMB requested agencies for the first time to provide information on the Privacy Act training provided to employees. It, among other things, requested data on (1) the number of employees that had received training, (2) the criteria used in deciding who was to receive training, and (3) whether the training was internal or external. This information, which may be available from personnel or other records, should be useful to OMB and the respective agencies in assessing Privacy Act training.

Agencies Need to Evaluate Privacy Act Activities

The six agencies maintain over 1,400 systems of records containing millions of records on individuals. As shown in chapter 2, they have highly decentralized delegations of responsibility for safeguarding the systems. Because of the sensitivity of the records and the organizational structures, periodic evaluations are necessary if agency management is to be aware of how effectively the operations are being carried out as well as areas needing improvement. However, Privacy Act officers were able to identify only five reviews relating to Privacy Act operations in four of the six agencies since 1980.

OMB's Guidelines Stress Internal Evaluations

The Privacy Act espouses the principle that there are proper approaches to the management of information and that agencies should take affirmative steps to assure that their information management practices conform to a reasonable set of norms. OMB incorporated this principle in its Circular Nos. A-108 and A-130.

OMB's Circular No. A-108, published in 1975, required each agency "to establish a program for periodically reviewing agency record-keeping policies and practices to assure compliance with the Act." Circular No. A-130, issued on December 12, 1985, more specifically concerned compliance evaluations. Among the provisions of appendix I to Circular No. A-130 are the following.

- Recordkeeping Practices. Review annually agency recordkeeping and disposal policies and practices in order to assure compliance with the act.

- Routine Use Disclosure. Review every three years the routine use disclosures associated with each system of records in order to ensure that the recipient's use of such records continues to be compatible with the purpose for which the disclosing agency originally collected the information.
- Matching Programs. Review annually each ongoing matching program in which the agency has participated during the year, either as a source or as a matching agency, in order to ensure that requirements are met.
- Privacy Act Training. Review annually agency training practices in order to ensure that all agency personnel are familiar with the requirements of the act, with the agency's implementing regulation, and with any special requirements that their specific jobs entail.

We discussed the Circular No. A-130 requirements with the OMB senior policy analyst who drafted them. He said the circular was issued to expand, clarify, and stress OMB's expectations for agency evaluations of Privacy Act functions. He said the circular was also intended to serve as an impetus for the agencies to emphasize internal reviews and provide sufficient priority to this function.

Agencies Have Not Emphasized the Review Function

Our work at the six agencies showed that emphasis has not been placed on evaluations of Privacy Act functions. Consequently, few evaluations have been conducted.

The following summarizes the evaluation efforts of each of the six agencies we reviewed.

- While Treasury's Privacy Act directive does not address compliance evaluations, the agency Privacy Act officer's position description includes the responsibility for "implementing and monitoring Departmentwide compliance with requirements of the Act." The Privacy Act officer said although compliance reviews have been planned, staffing constraints have forced postponement. The Privacy Act officer also said reviews were conducted at IRS as part of the National Office Review Program.
- Interior's Privacy Act officer cited two evaluations conducted in 1984. As part of Interior's triennial review program under the Paperwork Reduction Act, the agency assessed aspects of safeguarding Privacy Act systems of records. The assessment found deficiencies and made recommendations in the areas of (1) posting warning notices to limit access to areas where Privacy Act materials are maintained and (2) disposing of Privacy Act materials. In addition, pursuant to a request by a Member

of Congress, Interior reviewed selected aspects of the Privacy Act and Freedom of Information Act. The review identified areas where implementation and compliance could be improved including (1) improving the physical security and integrity of Privacy Act records and (2) notifying employees of the provisions of the Privacy Act, including its prohibitions. The Privacy Act officer told us that with only 30 percent of his time devoted to privacy matters he has been unable to conduct any reviews himself. He said that the agency's directive was revised in October 1984 to assign responsibility for onsite inspections to components and that some components began to conduct them in 1985.

- Labor's directive states that the Solicitor will (1) direct the overall implementation of the Privacy Act and (2) review disclosure officers' decisions periodically to assure adherence to Labor regulations. The senior Privacy Act staff member told us that she does not have the resources to conduct reviews of how the Privacy Act is implemented.
- VA does not have a comprehensive directive and its Privacy Act officer position description does not address evaluations. The Privacy Act staff was aware of two evaluations that were issued in 1980 and 1981. In 1981, the Privacy Act staff reviewed the Privacy Act systems of records of the Department of Veterans Benefits and found that improvements could be made in accounting for disclosures and in protecting confidential sources of information. In 1980, the Office of Inspector General issued a series of reports related to privacy and security controls of a major computer system. It reported the need for security audits and, at some installations, the need for Privacy Act training.
- Justice does not have a directive and its position description for the Privacy Act official does not include evaluation responsibility. The only review cited by officials was a 1983 internal audit report on the department's efforts to comply with the records protection requirements of the Privacy Act. It contained recommendations for the Justice Management Division (1) to more effectively monitor compliance with Privacy Act record security requirements and (2) to annually remind department components of their responsibility to identify records systems subject to the act and to prepare notices for those systems.
- HHS has delegated full responsibility for the Privacy Act's implementation to its major components. Our work at the SSA and the Health Care Financing Administration revealed that reviews of Privacy Act operations were not conducted. The Privacy Act officer at the Public Health Service told us that, at her suggestion, elements of the Privacy Act's implementation were incorporated into an internal control review conducted pursuant to the Financial Integrity Act. Through this effort she identified the need for improved Privacy Act instructions and training. According to the Privacy Act officer, corrective actions were being

taken. In January 1986, HHS created an ad hoc committee to review the administration of the Privacy Act and to make recommendations for improvements. Among the areas planned for review were computer matching, computer security, and the compatibility of HHS procedures with OMB guidance. On April 17, 1986, HHS officials told us that the committee was in the process of determining how to meet the review requirements contained in OMB Circular No. A-130.

Conclusions and Recommendations

Conclusions

The Privacy Act of 1974 is the principal statute aimed at balancing the privacy protection rights of individuals with the information needs of federal agencies in conducting government business. As such, it assures individuals that records about themselves will be safeguarded and kept confidential. The act also places disclosure, recordkeeping, and safeguarding requirements on federal agencies.

During the years since the act's passage, the number of government-held records has increased dramatically, and more records are automated each year. Automated records and the proliferation of microcomputers expand the uses and access to personal records and, thus present difficult privacy challenges that call for greater attention to Privacy Act requirements. However, the executive branch has not emphasized oversight of the Privacy Act. To fulfill its responsibilities under the act, OMB has adopted a reactive approach to oversight. Although this approach depends partially on following up on information provided by agencies for OMB's annual report to the Congress, 3 years elapsed between the publication of OMB's 1981 report and the December 1985 publication of the combined Privacy Act report for 1982 and 1983. The fact that OMB still has not published reports for 1984 or 1985 reflects the low priority it has given this program. At the same time, agencies have not emphasized oversight of their own.

Privacy Act activities are widely dispersed throughout agencies and their components. Consequently, the organizational structures established by agencies are decentralized in nature with primary reliance for compliance placed with local units that maintain and use individual systems of records. Given this decentralized approach, basic management tenets suggest the need for clear delegations that assign responsibility and establish accountability as well as a central focal point to monitor and oversee the law's implementation. Our analysis showed that this has generally not been achieved.

Agency directives and other memoranda that describe delegations for implementing the Privacy Act are unclear as well as incomplete. Of the 14 agencies reviewed, three did not have directives which formally delegated responsibilities. The remaining 11 delegated responsibilities through agency directives but did not address all Privacy Act provisions.

The role and functions of agency Privacy Act officers are less than needed to effectively coordinate and oversee the implementation of the

act. We found that significant functions such as ensuring compliance and necessary Privacy Act training were not always assigned.

Our detailed audit work at six agencies illustrated the need for closer attention to Privacy Act activities. Management in these agencies has been less than aggressive in reviewing initiatives to create new systems of records subject to the Privacy Act as well as decisions to automate existing systems. While OMB calls for detailed analyses to be conducted on potential risks and needed safeguards for new systems of records, we found they were rarely prepared by agency program staff. Privacy Act officers seldom inquired about risk assessments.

Although computer matching is one of the most controversial activities generating privacy concerns, agencies (1) did not have current, complete data on the extent of matching programs, (2) did not always follow OMB's matching guidelines, and (3) differed in interpretation of the matching guidelines as to whether programs needed to be reported to OMB. In addition, two component agencies exempted their matching programs from OMB's guidelines. We found no evidence that OMB was previously aware of these discrepancies. The Privacy Act officers were not always involved in computer matching activities.

While OMB guidance emphasizes the need to provide Privacy Act training to all personnel who handle Privacy Act records, agencies need a more systematic means to assess or provide for training. Given our findings that Privacy Act requirements and OMB guidelines are not being consistently followed in the areas of computer matching, risk assessments, and system automations, the need for agency personnel to become more aware of these requirements and guidelines is apparent.

In addition, the six agencies have not established systematic approaches for conducting compliance evaluations and providing management with feedback on Privacy Act activities. Privacy Act officers told us they do not have the resources to conduct evaluations themselves.

The pervasiveness of such shortcomings leads us to conclude that Privacy Act operations need a cohesive, articulated program aimed at assuring that such activities are conducted in full compliance with OMB guidance and the act's provisions. In our opinion, without more active involvement and monitoring by both OMB and agencies, there will be less than full assurance that Privacy Act functions are carried out in a manner that protects the privacy rights of individuals and balances these rights with the information needs of federal agencies.

OMB is currently planning to conduct a comprehensive review of its 1975 guidelines on implementing the Privacy Act. We believe this effort is timely in light of our findings. Revised guidelines with proper monitoring and oversight can address many of the needed improvements and emphasize the management responsibilities for implementing the act. But the full potential effect of revised guidelines, as well as Circular No. A-130, may not be realized without OMB leadership and active OMB oversight.

Recommendations

Because of OMB's key role in managing executive branch operations and in light of the responsibilities assigned OMB by the Privacy Act, we recommend that the Director, OMB, actively oversee agencies' implementation of the Privacy Act. This would entail following up periodically to ensure agencies' adherence to Circular No. A-130 and other OMB guidance.

Because needed changes will require strong leadership by agencies, we also recommend that OMB direct agencies to

- review and update (or in some cases, prepare) directives that clearly delegate responsibilities and establish accountability for all Privacy Act functions;
- specifically assign to the Privacy Act officers coordinating responsibilities for all Privacy Act activities and ensure that Privacy Act officers have the resources to fulfill these responsibilities;
- systematically assess and provide for Privacy Act training to assure that personnel are aware of Privacy Act requirements and OMB guidance pertaining to such functions as conducting detailed risk assessments, automating systems of records, and conducting computer matching programs; and
- assign responsibility for evaluating Privacy Act operations and monitoring implementation of any recommended improvements.

We also recommend that the Director, OMB, review and clarify OMB's guidance to agencies on automated systems of records and computer matching programs.

- Circular No. A-130's guidance on automating systems of records should provide more specific criteria on when agencies are to prepare a new system report and notice. This would result in greater consistency within and among agencies in recognizing the need to provide advance public notice and reports to OMB and the Congress.

- Computer matching guidelines should specifically state that agencies are to annually report to OMB all participation in matching programs initiated in prior years but conducted on a recurring basis. This would contribute to more complete data in OMB's Annual Report to the Congress.
- Computer matching guidelines should provide for public notice of computer matching programs conducted by organizations not covered by the act when Privacy Act systems of records are disclosed by federal agencies.
- Computer matching guidelines should instruct agencies to notify OMB when, like IRS and OCSE, they believe they are exempt from OMB guidelines. This would provide OMB with the opportunity to review and concur.

Agency Comments and Our Evaluation

OMB said that it found our recommendations to be reasonable and that it was already working to implement some of them. It additionally provided several comments which are discussed below.

OMB said the report should include a discussion of the Paperwork Reduction Act of 1980. The Paperwork Reduction Act established a broad framework for managing federal information resources and integrated many related functions, including privacy protection. OMB also said the report appeared to confuse the role of the senior agency official for privacy matters and the working level Privacy Act officer. In a followup discussion, OMB explained that, because Privacy Act functions are integrated with other information resource management duties, Privacy Act officers' activities may be supplemented by functions conducted by other groups such as agency Inspectors General and General Counsels.

We cited the Paperwork Reduction Act in the report. However, we do not believe OMB's comments are pertinent to our findings or recommendations. Under the Paperwork Reduction Act, OMB and agencies continue their responsibilities for implementing the Privacy Act. In fact, OMB's 1984 annual report under the Paperwork Reduction Act of 1980 stated:

"The Act emphasizes the importance of protecting personal privacy of individuals against unwarranted intrusions by Federal agencies and strengthens authorities previously assigned to OMB by the Privacy Act of 1974."

In addition, OMB's 1985 Circular No. A-130 entitled, "Management of Federal Information Resources," which provided a framework for information management including the implementation of the Paperwork

Reduction Act, continued and, in some instances, strengthened agency Privacy Act responsibilities.

We also agree that other agency activities supplement Privacy Act functions and the activities of the Privacy Act officer. As the report shows, Privacy Act activities are widely dispersed and include program staffs as well as other groups such as the General Counsel. Rather than solely focusing on the Privacy Act officer, we worked with this individual as a focal point and contacted many other groups where either the Privacy Act officer or agency documentation suggested their involvement. The fact that many other groups are involved in Privacy Act activities reemphasizes, in our opinion, the importance of a coordinating, focal point, such as the agency Privacy Act officer. These positions were established and located under the senior agency official for Privacy Act matters to coordinate Privacy Act implementation in the agency.

OMB said that time spent by Privacy Act officers in administering the Freedom of Information Act and other disclosure statutes may complement rather than compete with Privacy Act duties. We clarified the report to show that, because Privacy Act officers work on the Privacy Act part-time, their other duties must compete for time and resources regardless of whether the other duties are complementary or independent of Privacy Act responsibilities.

OMB questioned whether we found a relationship between the level of the Privacy Act officer in the agency and the accomplishment of his or her duties. We did not attempt to determine such a relationship. We did, however, include Privacy Act officers' locations and grade levels as part of our overview of how agencies have organized to implement the Privacy Act.

Letter Dated January 4, 1984, From the Chairman of the Subcommittee on Government Information, Justice, and Agriculture

GLENN ENGLISH, OKLA., CHAIRMAN
STEPHEN L. NEAL, N.C.
RONALD D. COLEMAN, TEX.
ROBERT E. WISE, JR., W. VA.
BUDDY MacKAY, FLA.
EDOLPHUS TOWNS, N.Y.

THOMAS N. KINDNESS, OHIO
TOM LEWIS, FLA.
DAN BURTON, IND.

(202) 225-3741

NINETY-EIGHTH CONGRESS

Congress of the United States
House of Representatives

GOVERNMENT INFORMATION, JUSTICE, AND AGRICULTURE
SUBCOMMITTEE
OF THE
COMMITTEE ON GOVERNMENT OPERATIONS
B-349-C RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, D.C. 20515

January 4, 1984

Mr. Charles Bowsher
Comptroller General
General Accounting Office
441 G Street, NW
Washington, D. C. 20548

Dear Mr. Bowsher:

This Subcommittee recently completed an investigation of the oversight of the Privacy Act of 1974 by the Office of Management and Budget. The Subcommittee's effort resulted in a report (House Report 98-455) adopted by the Committee on Government Operations at the end of the first session of this Congress. The report generally concluded that OMB's Privacy Act oversight efforts were deficient and recommended, inter alia, that there be better government-wide Privacy Act oversight and that there be better representation of privacy interests in government decision making.

Some of the problems with OMB's Privacy Act efforts may also be characteristic of Privacy Act activities at individual agencies. The regular review of system notices and proposed routine uses by the Subcommittee indicates that there may be organizational and other shortcomings with the way that agencies respond to Privacy Act requirements. While some agencies--most notably the Department of Defense--have model programs, other agencies place Privacy Act operational responsibilities at a low level, fail to give the agency Privacy Act officer a meaningful voice, or ineffectively coordinate Privacy Act issues among multiple agency components.

I would like to enlist the assistance of the General Accounting Office in reviewing the organizational structure and effectiveness of Privacy Act operations at major departments and agencies. The main purpose of this assignment is to determine if agencies have accorded sufficient institutional importance to Privacy Act matters to meet the requirements of the Act.

Mr. Charles Bowsher
January 4, 1984

In addition, I would like GAO to determine if major agencies are suitably organized to permit identification and consideration non-Privacy Act privacy issues in the ordinary course of agency business. My concern is that privacy matters that do not arise in the context of the Privacy Act or other specific legislation relating to privacy are not addressed.

Finally, I would like GAO to review the privacy policy activities of the National Telecommunications and Information Administration at the Department of Commerce. NTIA had been very active with privacy issues prior to 1981, and I want to know if privacy work is continuing at NTIA and, if not, why not.

Subcommittee counsel Robert Gellman can provide your staff with more information and direction with respect to this request.

Sincerely,

Glenn English
Chairman

Enclosure

Location and Resources of Component Privacy Act Staff

Agency/component	Organizational entity	Immediate office	Grade	Estimated staff years[a] Privacy Act officer[b]	Staff
Health and Human Services					
Health Care Financing Administration	Office of Management and Budget	Reports Management Branch	12	1	0
Office of Inspector General	Office of Analysis and Inspection	Management and Operations Division	15	.02	.05(1)
Office of the Assistant Secretary for Personnel Administration	Office of Personnel Administration	Division of Personnel Policy	12	.40	0
Public Health Service	Office of the Assistant Secretary for Health	Division of Directives and Authorities Management	14	.40	1(1)
Social Security Administration	Office of Operational Policy and Procedures	Division of Technical Documents and Privacy	15	.40	8.01(9)
Interior					
Bureau of Indian Affairs	Office of the Commissioner	Office of Administration	SES	.001	.30(1)
Bureau of Mines	Management Services	Division of Property and General Services	14	.05	.50(1)
Bureau of Reclamation	Office of Assistant Commissioner for Administration	Assistant Commissioner for Administration	SES	.03	.14(2)
Geological Survey	Administrative Division	Special Programs Section	13	.15	.05(1)
Minerals Management Service	Office of Administration	Records Management Branch	12	.10	0
National Park Service	Personnel and Administrative Services	Administrative Services Division	15	.02	2.05(1)
Office of Administrative Services	Division of General Services	Division of General Services	14	.01	0
Office of Aircraft Services	Office of the Director	Office of the Director	8	.03	0
Office of Inspector General	Assistant Inspector General for Administration	Assistant Inspector General for Administration	13	.05	.05(1)
Office of Personnel	Division of Program Coordination and Evaluation	Division of Program Coordination and Evaluation	14	.02	0
Office of Surface Mining Reclamation and Enforcement	Directorate of Budget and Administration	Division of Personnel	SES	.05	.20(1)
Office of Youth Programs	Administration Division	Associate Director for Administration	15	.01	.01(1)
United States Fish and Wildlife Service	Office of Assistant Director-Administration	Regulations and Management Review Branch	14	.01	.04(2)
Justice					
Bureau of Prisons	Office of General Counsel	Office of General Counsel	13	.40	.75(1)
Civil Division	Office of Deputy Assistant Attorney General, Office of Immigration Litigation, Office of Consumer Litigation, Executive Office, and Freedom of Information and Privacy Acts Unit	Freedom of Information and Privacy Acts Unit	13	.30	.90(3)

Agency/component	Organizational entity	Immediate office	Grade	Estimated staff years[a]	
				Privacy Act officer[b]	Staff
Civil Rights Division	Executive Office	Freedom of Information/ Privacy Acts Branch	11	40	4.35(9)
Executive Office for U.S. Attorneys	Legal Services Division	Legal Services Division	15	20	3.15(9)
Immigration and Naturalization Service	Office of the Associate Commissioner- Information Systems	Information Services Branch	14	50	3.10(14)
Land and Natural Resources Division	Office of Deputy Assistant Attorney General	Policy, Legislation and Special Litigation Section	15	01	03(2)
Office of Information and Privacy	Office of Information and Privacy	Office of Information and Privacy	15	20	30(27)
United States Marshals Service	Office of Legal Counsel	Freedom of Information/ Privacy Act Office	14	95	1.50(3)
Labor					
Employment Standards Administration[c]	Office of Management, Administration and Planning	Branch of Office Services	12	05	02(2)
Office of Inspector General	Office of Inspector General	Office of Inspector General	14	10	10(1)
Office of the Assistant Secretary for Administration and Management[c]	Directorate of Information Resources Management	Office of Information Management	13	01	0
Treasury					
Bureau of the Public Debt	Office of the Commissioner	Office of the Commissioner	14	10	10(1)
Internal Revenue Service	Associate Commissioner for Policy and Management	Disclosure and Security Division	SES	05	30(3)[d]
Office of Inspector General	Office of Inspector General	Office of the Director for Administration	12	80[e]	0
Office of the Comptroller of the Currency[f]	Office of the Chief Counsel	Legal Advisory Services Division	14	20	0
	Deputy Comptroller for Industry and Public Affairs	Communications Division	13	03	03(1)
U.S. Customs Service	Office of Commercial Operations	Disclosure Law Branch	15	25	2.50(5)
Veterans Administration					
Department of Medicine and Surgery	Office of the Assistant Chief Medical Director for Administration	Medical Administration Service	SES	05	55(2)
Department of Veterans Benefits	Administrative Services Staff	Administrative Services Staff	14	15	1.40(6)
Office of Inspector General	Office of Assistant Inspector General for Policy, Planning and Resources	Policies and Procedures Division	SES	05	75(2)

[a]The first column represents the Privacy Act officer's time spent on Privacy Act functions, the second column represents the staff's estimated time spent, and the number in parentheses is the total number of staff available.

[b]Identified by the agencies as being the focal point for Privacy Act coordination and/or oversight. These individuals have various titles. For purposes of this report we refer to them as component Privacy Act officers.

[c]Does not include resources devoted to access and disclosure requests by disclosure officers.

[d]Figures include Privacy Act officer and immediate staff. However, according to an IRS official, the time for the Privacy Act officer and staff in the National Office and field locations cannot be appropriately broken down between Privacy Act duties, related activities which support, duplicate, or supplement the Privacy Act; and privacy issues not covered by the act. Consequently, the full operation involves an estimated 292 staff years.

[e]Includes Freedom of Information Act duties. Privacy Act officer said she could not separate these from Privacy Act duties since all first-person requests involve both acts.

[f]At the Office of the Comptroller of the Currency, no single Privacy Act officer has been formally designated. Legal and administrative responsibilities are assigned to a senior attorney and a public affairs specialist, respectively.

Comments From the Office of Management and Budget

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

JUN 23 1986

Mr. William J. Anderson
Director
United States General
Accounting Office
Washington, D.C. 20548

Dear Mr. Anderson:

This is to confirm and reiterate the analysis of your draft report, "Privacy Act: Federal Agencies' Implementation Can Be Improved," provided to your staff orally by Robert N. Veeder of my staff.

The main points we wish to emphasize are these:

- The report does not address the effect of the Paperwork Reduction Act of 1980 on both the agencies' implementation of the Privacy Act of 1974 and OMB's oversight responsibilities. We think this is a serious omission.

- In the discussion of the role of the departmental Privacy Act officer, the report appears to confuse the role and responsibilities of the senior official and the working level privacy officer. Again, we think it is important to address the Paperwork Reduction Act dimension here.

- In analyzing the percentage of time PA officers spend on non-privacy matters, we think it is important to note that the time they spend administering the Freedom of Information Act or other similar disclosure or confidentiality statutes is time spent in a complementing and not necessarily competing activity.

- We also think that the section analyzing the role of the Privacy Act officer needs a bottom line: is there a relationship between the level of the PA officer and the accomplishment of his or her duties? We also note parenthetically that the report, in focusing solely on the PA officer, misses opportunities to document other ways in which the Act is implemented - i.e., what is the role of the Inspector General or the General Counsel?

As to the recommendations, we think they are reasonable in light of the report's findings. Some, in fact, we have been working to implement.

Thank you for the opportunity to comment on the draft.

Sincerely,

Wendy L. Gramm

Wendy L. Gramm
Administrator for Information
and Regulatory Affairs

Glossary

Computer Matching Program	Not addressed by the Privacy Act, but OMB defines it as "a procedure in which a computer is used to compare two or more automated systems of records or a system of records with a set of non-Federal records to find individuals who are common to more than one system or set. The procedure includes all of the steps associated with the matching program, including obtaining the records to be matched, actual use of the computer, administrative and investigative action on the hits, and the disposition of the personal records maintained in connection with the program. It should be noted that a single matching program may involve several matches among a number of participants."
Hit	Defined by OMB as the identification, through a matching program, of a specific individual.
Matching Agency	Defined by OMB as the federal agency which actually performs the matching program.
Notice of Match	OMB matching guidelines call for matching agencies to publish in the Federal Register a brief notice describing the matching program which includes the following items. 1. The legal authority under which the program is being conducted. 2. A description of the matching program including whether the program is one time or continuing, the organizations involved, the purpose(s) for which the program is being conducted, and the procedures to be used in matching and following up on the "hits." 3. A complete description of the personal records to be matched, including the sources(s), system of records identifying data, date(s) and page number(s) of the most recent Federal Register full text publication where appropriate. 4. The projected start and ending dates of the matching program. 5. The security safeguards to be used to protect against unauthorized access or disclosure of the personal records.

	6. Plans for disposition of the source records and "hits." Agencies should send a copy of this notice to the Congress and to the Office of Management and Budget at the same time it is sent to the Federal Register.
Record	Defined by the Privacy Act as "any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph."
Report on New System (RONS)	In its Circular No. A-130, OMB established criteria for agencies to determine when a RONS must be submitted to it and the Congress. OMB also specified the content of the report to include a brief narrative statement which (1) describes the purpose of the system, (2) identifies the authority for maintaining the system, (3) provides the agency's evaluation of "the probable or potential effect of such proposal on the privacy and other personal or property rights of individuals or the disclosure of information relating to such individuals and its effect on the preservation of the constitutional principle of federalism and separation of power" (required by the act), and (4) provides a brief description of steps taken by the agency to minimize the risk of unauthorized access to the system of records including a discussion of higher or lower risk alternatives which were considered for meeting the requirements of the system. A more detailed assessment of the risks and specific administrative, technical, procedural, and physical safeguards established is to be made available upon request.
Risk Assessment	OMB requires that a Report on New System include a brief description of steps taken by the agency to minimize the risk of unauthorized access to the system of records. A more detailed assessment of the risks and specific administrative, technical, procedural, and physical safeguards established is to be made available upon request.
Routine Use	Defined by the Privacy Act as "with respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected."

Safeguards	The Privacy Act requires agencies to "establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained."
Source Agency	Defined by OMB as the federal agency which discloses records from a system of records to be used in a computer matching program.
System Notice	The Privacy Act requires each agency to publish in the Federal Register a notice of the existence of each system of records which includes: 1. the name and location of the system; 2. the categories of individuals on whom records are maintained; 3. categories of records; 4. routine uses; 5. agency policies and practices for storage, retrievability, access control, and disposal of records; 6. the title and business address of the agency official responsible for the system; 7. procedures for notifying individuals of records maintained on them; 8. agency procedures on how individuals may gain access to records kept on them in a system of records; and 9. categories of sources of records in the system.
System of Records	Defined by the Privacy Act as a "group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

Written Agreements

OMB matching guidelines state "prior to disclosing to either a Federal or non-Federal entity, the source agency should require the matching entity to agree in writing to certain conditions governing the use of the matching file, e.g.: that the matching file will remain the property of the source agency and be returned at the end of the matching program (or destroyed as appropriate); that the file will be used and accessed only to match the file(s) previously agreed to; that it will not be used to extract information concerning 'non-hit' individuals for any purpose; and that it will not be duplicated or disseminated within or outside the matching agency unless authorized in writing by the source agency."

Requests for copies of GAO reports should be sent to:

U.S. General Accounting Office
Post Office Box 6015
Gaithersburg, Maryland 20877

Telephone 202-275-6241

The first five copies of each report are free. Additional copies are $2.00 each.

There is a 25% discount on orders for 100 or more copies mailed to a single address.

Orders must be prepaid by cash or by check or money order made out to the Superintendent of Documents.